	DISPOSITION OF PUBLIC COMMENTS ON DRAFT POLICY STATEMENT ANM-03-117-9	
Commenter	**Comment**	**Disposition**
Raytheon 3/24/03	Example 6: An electronic system with a manual safety feature. The discussion using ARP 4754 guidance would be more informative if the YDM malfunctions were classified as Major rather than Hazardous in this example. Looking at this example from the software aspect only. It would seem that the switch because it is a simple device, without any software, would by definition have a software DAL of A. That is there are no software design errors that can cause this switch to malfunction. If this is the case, then cannot the software DAL for the YDMs correspond to the most severe failure condition associated with YDMs? For example, if the dutch roll oscillations due to YDMs was classified as Major then the software DAL would be C. The reference to ARP 4754 para 5.4.1.2. when discussing DAL of switch in the section implies that this may not be acceptable. Unless this is related to Hardware DAL.	Assigning DAL should be approached from the system point of view, and should not be looked at only from the s/w angle alone (or h/w alone for that matter.) If the h/w is governed by the system requirements, so should be the s/w. Even if the YDM failure alone is classified as Major, because the switch failure probability is relatively high, it would be more conservative to assign level B to the YDM. The ARP takes this conservative approach in allowing only one development level below the system top level hazard category which in this example is Catastrophic. Disposition: Example 6 will remain as originally written.
Rockwell Collins 3/27/03	**1) Section B. Policy Derivation** **Subsection (1), Main Differences Between the Guidelines**, second paragraph under 'Scope': "The hardware safety assessment, the functional hazard assessment (FHA), the preliminary system safety assessment (PSSA), and the system safety assessment (SSA) processes are used in combination to determine the hardware DALs." Rockwell Collins contends that use of the SSA process to determine hardware DALs is too late in the development process and therefore the SSA process should not be included in the statement above.	1) **Subsection (1), Main Differences Between the Guidelines** Comment relates to the 3rd paragraph under Scope. For large scale projects, it is very true that the SSA is done later in the process and it verifies, rather than determine, the DALs. However, for small scale STC projects, it may be possible to use the SSA as the final determination of the DAL. Further, DO-254, section 2.2 does mention the use of SSA in allocating DAL to h/w. Disposition: Revise memo to say: The hardware safety assessment, the functional hazard assessment (FHA), the preliminary system safety assessment

		(PSSA), and, *as time permits*, the system safety assessment (SSA) processes, are used in combination to determine hardware DALs.
	2) **Subsection (2), Application Examples** a) Example 1b: Partitioned Design – This discusses an architecture where there are dual channels, each containing command and monitor functions. The guidance seems to state that the Command function should be Level A and the Monitor function should be Level C. It is noted under ARP-4754 that the switching/voting detection function should be Level A. Thus, it would seem that the Command would be performing the detection based on disagreement with the monitor function. Therefore, the monitor is not active. It just seems to provide an output for comparison. This is backward from the way manufacturers normally think of the Command/Monitor architecture. Usually, the Monitor function does the detection and switching/shutdown/etc. and is the highest level. This is because the Monitor function is usually less complex than the Command function and thus, is more cost effective to make the Monitor function Level A. This example could cause difficulty for an applicant if an ACO ASE follows this guidance to the letter. Rockwell Collins perceives Example 4 as an acceptable approach to a command and monitor architecture. b) Example 2: Parallel Architecture (dissimilar and	2) **Subsection (2), Application Examples** a) Example 1b: there is no preference in this example what the DALs should be for command or monitor function. The manufacturers have the flexibility to assign level A to either function. The FAA does not have a preference or requirement that the command side must be assigned higher criticality. In either case, it is important that the DAL assignment is consistent with the PSSA. Disposition: No change. b) Example 2: If DO178B alone is used as guidance

	independent) – The conclusion in this example seems to be that in taking the architecture into consideration, a function with catastrophic results could be implemented using Level B compliant software. This seems to be allowing 2 functions at Level B to be equivalent to Level A which is inconsistent with current FAA software guidance, for avionics systems, at least, and should be confirmed or removed.	for avionics, then at least one portion is level A. This is the biggest difference between the ARP and 178B as 178B does not allow credits for dissimilarity and independence aspects in a system architecture. With ARAC's 25.1309 recommendation of using the ARP4754 as the starting point for DAL assignment, the dissimilarity AND independence in an architecture can indeed be taken into account when assigning software levels. Justifying dissimilarity and independence is not a trivial task, however, and must be thoroughly investigated before credits can be taken. Disposition: No change.
	c) Example 3: Parallel Architecture (redundant channel) – This example discusses a system that has a primary and a secondary channel that provide the aircraft function. The secondary is not used unless the primary has failed; it does not contribute to failure detection and cannot cause the primary to fail. The FHA states the effect of a combined malfunction as being catastrophic and the effect of individual channels as major. Rockwell Collins requests clarification on this example. If the primary channel is always used, then does it detect its own failures or is that accomplished outside this function? If the primary channel fails, then does the secondary channel provide the function alone? If the latter is the case, then the secondary channel is now providing a function with catastrophic failure	c) Example 3: To answer RC's question, a simple display system will be used to help illustrate the concept. The primary displays are dissimilar from the standby, but they are not entirely independent from the standpoint that the air data system employs identical probes. -The primary displays do not detect own failures. The detection is done by the crew. -The standby will provide the function when the primaries fail (assume both pilots displays fail concurrently.) -Failure of primary plus standby is Catastrophic, but either failure is by itself Major. -The primary displays are level A. -The standby display should be level B per the ARP (level C might have been accepted in the

	effects. How can the failure effect of the individual channel be only major? Normally, in a redundant channel situation, both the primary and the secondary channel must be at the highest criticality level. If the failure effect is catastrophic, then the SW in both should be developed to Level A. For this example, the Summary concludes that one of the channels should be Level B. Rockwell Collins questions how the secondary channel can be at a different level from the primary channel. Whether one concludes Level B or Level C is appropriate, it has not been acceptable to the ACO in the past d) Example 5: Backup Parallel Architecture – Again the backup is a different software level then the primary channel. It does state that the channels are independent and there can be no common mode failures. Rockwell Collins requests clarification on how the backup channel can be a lower criticality level if it is intended to perform the same function as the primary channel when the primary fails. If the effect of a malfunction is catastrophic, then it should be Level A as well as the primary. e) Example 7: Mechanical System with Software Controlled Safety Feature -This example has a hardware air duct with a10^{-7} failure rate. If the air duct bursts, the	past.) Judging by the questions, it appears RC is only considering a double failure scenario, or that the two channels are of the same design which is not the scenario intended by Example 3. Disposition: No change. d) Example 5: It is recognized that when the primary channel is loss, and the backup channel is activated, the airplane is operating at a higher level of risk. This higher level of risk should be temporary because full system capability should be restored within an acceptable period that is identified in the safety analysis. This concept is true with hardware, and is equally applicable to s/w. If the s/w level is based strictly on DO-178B guidance, where system architecture is not always given credit, and where the term “contribute” has lead to more conservative assignment of software level than is needed to meet the regulation, as discussed under section A of the Appendix. Disposition: No change. e) Example 7: In this example, a duct burst in and of itself is NOT catastrophic. The catastrophic condition occurs only when the duct burst in

	result is catastrophic. This failure is protected by a software function that, according to this policy memo, could be developed to Level C. This appears to be inconsistent with current FAA policy and established Industry practice. **General Policy Comment:** This policy discusses application of DO-254 at a "component", i.e. LRU level, whereas the FAA's draft advisory circular for adoption of DO-254 is limited to application only at a "component", i.e. piece part level. This apparent divergence should be clarified.	combination with the inability to isolate the hot air flow. According to the ARP, it is acceptable to have the monitor s/w level to be lower than the top event, provided the combination of failure meet the top level requirement. This is in line with Example 4, which RC has perceived to be an acceptable approach. Disposition: No change. f) General Policy Comments: The policy can be applied equally to an LRU or its subcomponents. Further, LRU level DAL assignment is normally identical to the assignment at the "piece part" level. There is no divergence. Disposition: No change.
RCS	**1.0 GENERAL COMMENTS** a) This policy memo recognizes the importance of system architecture in the determination of appropriate design assurance levels (DALs) for hardware and software components of that system architecture. It also recognizes the important differences in the guidance contained in SAE ARP4754, RTCA/DO-178B, and RTCA/DO-254 for determining the appropriate DALs for hardware and software. This policy memo establishes a standardized approach to the use and application of these guidelines and industry practices. Such a standardized approach is extremely important and valuable for the aerospace industry. b) The standardized approach promoted by this policy	1.a) Thank you. 1b) STC should be treated on a case-by-case basis depending on the scope of the change. If a STC interacts with the TC design in such a way that there is a lack of system separation when required or that failure propagation/isolation becomes a safety issue, then the STC should not be approved. If the STC fundamentally changes the architecture of the original TC system, then the DALs might have to be completely reassessed or reassigned. If the STC addition is properly segregated from the TC design, then it should be feasible to assign DAL within the STC context. In any case, the policy guidance is equally applicable.

	appears to focus primarily on 14 CFR Part 25 Type Certificated (TC) airplanes. However, Supplemental Type Certificated (STC) projects represent a large fraction of the total number of airplane projects handled by the FAA and JAA every year. STC systems pose interesting problems for DAL determination. The addition of new functionality represented by the addition of a new system is constrained by the systems architectures and systems components DAL assignments of the Type Certificated airplane systems supporting and interacting with the new system addition. The STC system cannot readily impose changes on the DAL assignments of existing components. The DAL assignments of the STC system's components could potentially undermine or negate the DAL assignments of the existing TC airplane's systems. There is no guidance available to 14 CFR Part 25 STC applicants to steer them in the right direction in these situations. The policy memo should include some discussion of the application of the policy to STC systems and one or more examples of the DAL determination for STC systems added to a TC airplane. c) The policy appears to imply the FAA will dissuade applications from using triple channel identical hardware / identical software systems architectures for airplane-level functions with catastrophic hazards due to malfunction or loss of function if the applicant attempts to use RTCA/DO-178B Level A and RTCA/DO-254 Level A DALs for software and hardware, respectively. Applicants are to be persuaded to use dissimilarity in architectures in conjunction with Level A DALs if such levels are still necessary with the use of dissimilarity. This is a sharp departure from previously certified	Disposition: No change required. 1c) Surmising that RCS is referring to policy statement number 3, there is no intent to dissuade identical redundant channels with level A assignment. On contrary, the FAA continues to dissuade reliance on dissimilarity. However, if an applicant would like to take credit for the extra effort of establishing system dissimilarity AND INDEPENDENCE (not a trivial task), then it may be possible to reduce the DAL (per example 2.) Please note that dissimilarity and independence are two different aspects, and the existence of one does not imply the existence of the other. Disposition: No change required. 1d) RCS suggestion to clarify airplane-level function(s), functional allocations made to the system architecture's major components, and allocations made to hardware verses software in those major components are addressed in Examples 6 and 7 which are "real life" situations with minor editing to protect proprietary information. RCS comments on random hardware faults, manufacturing errors, physical treats, etc., appear to refer more to common cause analysis than to DAL assignment decision making, the latter is the main objective of the policy memo. Disposition: No change required.

	systems such as autopilots. d) The examples illustrating the application of the new policy in contrast and comparison to the applications of guidance from SAE ARP4754, RTCA/DO-178B, and RTCA/DO-254 for determining the appropriate DALs should be clarified to explain a) the airplane-level function(s) supported by the example, b) the functional allocations made to the system architecture's major components (i.e. parallel channels, or command and monitor channels, or primary and standby channels) in the example and c) the functional allocations made to hardware verses software in those major components. It is also important to discuss whether a system, software, or hardware DAL is addressing random hardware faults, system design errors, software design errors, hardware design errors, manufacturing errors, physical threats, operational errors, environmental conditions, or other conditions that can result in the hazards. **2.0 SPECIFIC COMMENTS** **RELEVENT PAST PRACTICE** Paragraph 5: The common use of the term DAL for ease of readability is understood, however, in using this common term and by the further comparing and contrasting within the Policy Statement of ARP4754, RTCA DO-178B and RTCA DO-254 confusion as to the original intent of each of these documents begins to enter in. The policy does not make it clear that there is a hierarchy within these documents and that they are intended to be used hand in hand to collectively assign Development	Relevant Past Practice – Paragraph 5: Industry has not formally established any "hierarchy" between the 3 documents other than the ARP4754 is a system level guidance, DO-178B is for s/w, and DO-254 is for hardware. Perhaps this lack of hierarchy greatly contributes to the "endless" discussions between applicants and FAA about DAL assignments. However, it is not appropriate for this policy memo to unilaterally claim such hierarchy. The policy memo does imply a <u>preferred</u> approach of using the ARP4754 as the starting point for DAL discussion, while still allowing applicants the choice to use DO-178B for s/w level assignment and not take any credit for the system architecture. There is

	Assurance Levels, Design Assurance Levels, Software Levels and provide the detailed guidelines necessary to achieve the associated objectives of each. **POLICY**	less ambiguity between the ARP and DO-254 with respect to h/w DALs. Disposition: no change.
	1. There is no common understanding within industry and the FAA regarding the level of effort or analysis required for systems which are expected to have worst-case failure conditions of "Minor" or "No Safety Effect". Recent mishaps indicate applicants do not consistently apply a minimum level of analysis (i.e. FHA and PSSA) to such systems, which can lead to disastrous results. It would be helpful to industry and to the FAA to insure consistent application of this minimum analysis effort early in the systems certification process, by explicitly stating that the system FHA and PSSA must be correctly performed for any certificate applications, including those for Minor and No Safety Effect systems. Recognition of ARP4754 (thus Table 5) provides some clarification on this.	Policy 1. RCS comments regarding correct safety analysis even for Minor or No Safety Effect events are well taken. However, it is not the main intent of this policy memo to establish policy for PSSA or SSA. Disposition: no change.
	2. "Redundant systems" as used in this section implies two or more systems that work together. However, this point appears to address a single system intended to implement a function, whose systems architecture consists of two or more identical and thus redundant elements. This sentence should be rewritten as "This method, particularly when applied to a system architecture with redundant elements, may result in a more conservative assignment of the DALs to the redundant elements than is necessary to comply with §§	2. Suggestion accepted. Disposition: revise affected sentence to read: "This method, particularly when applied to a system architecture with redundant elements, may result in a more conservative assignment of the DALs to the redundant elements than is necessary to comply with §§ 25.1301 and 25.1309."

	25.1301 and 25.1309." 3. The draft policy memo wording implies it is acceptable to address potential common-mode design errors across system architecture components using Level A DALs if the common-mode failure results in a catastrophic hazard, and that such components should be assigned Level A DALs. However, Level A DAL assignment would be mandatory (a "must", not a should) in such a situation. This policy statement indicates that the ACO ASE should recommend the common mode design error be addressed architecturally as a preferred solution to address the common mode design errors. It is also important to discuss whether a system, software, or hardware DAL is addressing random hardware faults, system design errors, software design errors, hardware design errors, or other conditions that can result in hazards (manufacturing errors, physical threats, operational errors, environmental conditions, etc.). For example, existing regulatory guidance discusses addressing common mode design errors that can result in catastrophic hazards either with Level A DALs for the system, hardware, and software, or with dissimilar designs. This policy ought to address common mode design errors in systems that can produce catastrophic hazards. Specifically, which techniques are acceptable means of precluding such errors? Is it adequate to use level A DALs, without hardware dissimilarity, to use hardware dissimilarity with reduced DALs, or are both means required? 4. This policy statement starts out with the statement that ARP4754 may be used to assign DALs for a system and	3. Although the intent for a level A is a "must" instead of a "should" as required by the safety analysis, within the context of a policy memo, the use of "must" may be legally interpreted as rule making which is not appropriate. Regarding the large issue of common causes, again, it is not the purpose of this memo to establish how general common cause failures should be mitigated, other than to affirm that level A (in case of catastrophic) is acceptable, or if the design provides a clear architectural mitigation then DAL credits may be appropriate. 4. It is not clear what RCS means by "architectural components." Please explain.

	its hardware and software components. After all the criteria are applied, per the policy statement, the final decision gate leads to the use of policy 2 or RTCA DO-178B for DAL assignment. This seems to indicate that system and hardware are assigned DALs by RTCA/DO-178B, but RTCS/DO-178B is specifically intended for software development not system or hardware development (reference B. POLICY DERIVATION (1) Scope 2nd sentence). It is also suggested that the sentence "The guidance of SAE ARP4754 may be used to assign DALs for a system and its hardware and software components" be replaced with "The guidance of SAE ARP4754 may be used to assign DALs for a system, its architecture components and their hardware and software." Additionally, the sentence " If the criteria of the SAE ARP4754 are not satisfied, the DALs may need to be assigned a higher level using the direct assignments of policy 2 above or using the guidance of RTCA DO-178B" be replaced with "If the criteria of the SAE ARP4754 are not satisfied, the DALs assigned to the architecture components and their hardware/software may need to be assigned a higher level using the direct assignments of policy 2 above or using the guidance of RTCA DO-178B."	
	5. It is important that the differences between RTCA/DO-178B and SAE ARP4754 on software DAL determination perceived by the applicant be presented to the cognizant ACO for concurrence before the applicant proceeds with software development and systems development and integration. This activity should be a decision point/gateway early in a project to preclude the applicant from presenting a position at odds with the	5. RCS comments are well taken. Early ACO concurrence is addressed in policy statement 1.

	ACO's understanding of the perceived differences at the end of software development and systems integration. At that point the applicant may argue the undue economic impact of redeveloping the software runs counter to the FAA's charge of promoting aviation business activity. 6. No Comments. **EFFECT OF POLICY** It is stated, "The office that implements policy should follow this policy when applicable to a specific project". Explicit guidelines outlining as to when this policy is applicable to a project would be helpful in this paragraph. **EXAMPLE 4: Active-Monitor Parallel Architecture** <u>Safety Assessment Column</u>: Under the FHA => Effect of failures of Sa alone – It is stated that Malfunction = Hazardous (would be catastrophic without the monitor). A note here stating that it has been determined to be Hazardous due to a failure condition not constrained by the monitor would help alleviate confusion as to why this is not driven by loss of function due to the monitor catching the malfunction and removing (loss) the function which is stated to be Major. This example illuminates the inherent differences between assigning DALs to hardware and to software. As stated, in the DO-178B column, "The guidance does not discuss what Sm	This is a canned legal statement. It allows an interpretation that a policy statement is not binding (unlike a FAR.) Disposition: no change. Example 4: to eliminate confusion with the loss of the system which is categorized as Major, the individual effects of Sa and Sm will be revised as follows: Disposition: change classification of -Malfunction of Sa alone to Major -Loss of Sm alone to Major The FAA does not have a preference between the command and monitor channel with respect to which of them should have higher DAL. RCS comment on the difference between h/w and s/w DAL assignment is noted. To avoid unnecessary debate, the sentence will be removed. Disposition: delete sentence ""The guidance does not

	software level should be if Sa is developed to Level A". This is due to the fact that the Safety Monitoring technique is used to allow a reduction of software level of the monitored function (to the level associated with the loss of the related system function). Developing Sa to Level A with this technique would defeat the purpose of utilizing the Safety Monitoring architecture. Note: Typo in column header for RTCA DO-178B **EXAMPLE 5: Backup Parallel Architecture** The findings of the FHA do not make sense in this example or at least make the reader fill in a bunch of assumptions. Since this is a backup architecture, Sb will only come "on-line" after loss of Sa. Is the FHA description for "Effect of Sa alone: Hazardous" for Malfunction or loss or both? Same for "Effect of Sb alone". Note: Typo in column header for RTCA DO-178B	discuss what Sm software level should be if Sa is developed to Level A." from the DO-178B column. Correct the typo in column header by changing RTAC to RT**CA**. Comments well taken. Disposition: revise as follows: -Under FHA: -Effect of Sa alone: Hazardous (malfunction) -Effect of Sb alone: Minor (loss) -Correct RTCA DO-178B column header.
Rolls-Royce	1) The summary of the document should state that whenever DO-178B and ARP4754 disagree about which level to use, select the ARP level. When the policy is agreed it should be fed into RTCA and EUROCAE for consideration at the next revision of DO-178, which I understand is planned for next year. 2) I would like to see some guidance on systems that can be dispatched with portions failed (Time Limited Dispatch). For example, a system where an AND gate of 3 events feeds into a Catastrophic top-level condition. When dispatching full-up, it may be acceptable to have A, B and C, for the levels of the 3 portions. However, dispatch with the first one failed (leaving just a B and a C) might not be permissible. What about dispatching with the second one failed, leaving A and C, etc?	1) One purpose of the memo is to recognize the ARP4754 method of assigning DAL, in addition to the DO-178B method if a applicant chooses it. Policy statement 5 provides the guidance for when the ARP4754 and DO-178B disagree. SAE and EUROCAE are aware of the proposed policy. Disposition: No change to policy memo. 2) The decision to allow which failures to dispatch is not the subject of this memo. There is a plan to discuss TLD as part of the more generic subject of "specific risk" in Phase 2 of ARAC activities on 25.1309. The FAA expects the issue being raised by RR will be discussed thoroughly at that point. For

	3) In example 4 it states that a nuisance shut down is Major whereas JAR-E (ACJ E 510, 2.1) clearly states that IFSD is only Minor. 4) Can we have clarification of what standing the policy will have when it comes to updates. For example, if a system has been developed to level C (in accordance with DO-178B) and certified, and is subsequently updated after the policy has been issued, might it subsequently have to be developed to level B (per examples 2, 3 or 4) or could grandfather rights be claimed?	now, this policy memo will not be extended to cover that issue. Disposition: No change. 3) Example 4 depicts an Active-Monitor architecture (command and monitor.) This example is not an engine shutdown scenario. Disposition: No change. 4) Assuming the update does not fundamentally change the system functionality or criticality, then the existing DAL can be used. This is one reason for policy statement 5 to say that DO-178B may continued to be used to determine s/w levels. Disposition: No change.
Boeing	The proposed policy statement provides a brief history, the proposed itself, and an appendix with a description of the issues and an explanation of the policy derivation with seven hypothetical examples. The examples in the draft policy statement would benefit from clarification of the Functional Hazard Assessments (FHAs) and Preliminary System Safety Assessments (PSSAs) and further development of the application of RTCA DO-254. Once the examples are clarified, further elaboration of the issues is needed in order to refine the policy statement, particularly that leading up to policy Item 6 regarding RTCA DO-254. Our specific comments on the issues and examples contained in the appendix to the policy statement that were used to formulate the policy are contained in the enclosure to this letter. Our specific comments on the policy itself are as follows:	• Item 1: suggestion to change the word "components" to "items" accepted. Disposition: change word as requested. • Item 3: suggestion accepted. Disposition: change sentence to read: "If a design could contain potential common-mode design errors…" • Item 6: If taken to its logical conclusion, it appears the comment implies the ARP4754, which deals with the development at the system level, could potentially be replaced by the methodology in DO-254. Although this concept may have merit, it requires a very significant "paradigm" shift in the way industry

	• The last word of the first sentence of Item 1 of the proposed policy should be changed from "components" to "items." This change would make the wording consistent with RTCA DO-254 and would avoid the ambiguity of the term "components" which is often used when considering individual parts of an electronic circuit. • The first sentence of Item 3 of the proposed policy statement should be modified from "If a design contains common mode design errors…" to "If a design could contain potential common-mode design errors…" This change should be made because the design assurance levels are determined as a function of the potential for errors and their consequences, not the errors themselves, which one seeks to avoid. • Item 6 of the proposed policy statement inaccurately describes the guidance of RTCA DO-254 as being applicable to electronic devices. The guidance in that RTCA document applies to functions implemented in complex electronic hardware, rather than devices in particular. This distinction is important, as it helps keep the guidance from becoming obsolete as electronic technology evolves, and it facilitates the application of a safety-oriented design assurance strategy to be applied to a variety of electronic technologies through a Functional Failure Path Analysis, when needed, that is not inconsistent with SAE ARP 4754. The proposed policy statement, as written, is incomplete regarding application of DO-254, particularly for using it to determine DALs. The policy should eventually reflect the flexibility afforded by DO-254 when justified by a safety assessment.	understands and applies these two documents in that industry generally looks at DO-254 as applicable only to the h/w level. The implied concept contained in the comment is above and beyond the scope of this policy memo and it should be discussed within the context of the proposed AC 20-XX. An alternative is to bring this discussion directly to the SAE S-18 committee as well as to RTCA before it can be turned into FAA policy. Disposition: no change to policy number 6. Suggest Boeing initiate such discussion to introduce their idea to industry.

	In summary, we recommend that the FAA continue development of this policy before implementing it. We would welcome further opportunities to discuss it in order to clarify the complex issues involved.	• Summary: The intent of this memo is consistent with ARAC recommendations (reference proposed AC 25.1309-1B, a.k.a. "Arsenal version) which clearly prefer the use of APR4754 as the leading guidance for DAL assignment. At this point the FAA does not see a need to hold up the issuance of this memo for the purpose of "continue development." As FAA and industry's thinking evolves with more experience in applying the ARP4754 as well as DO-254, it is possible that new or revised policy may be appropriate.
Boeing	**Comments on Section A: THE ISSUES** The last paragraph of Section A should be revised to reflect DO-254 rather than say that DO-254 "contains its own recommendations for electronic design assurance levels." This implies that its "own" recommendations are without regard for SAE ARP 4754 and does not acknowledge that DO-254 presents an extension of the PSSA methods in SAE ARP 4754 with an enhancement. This enhancement accommodates an explicit correlation of a functions safety assessment and its DAL when using a Functional Failure Path Analysis rather than assigning a predetermined lower DAL per SAE ARP 4754 Table 4 (which may or may not explicitly correlate with the safety assessment of the function). Ultimately, RTCA DO-254 is consistent with SAE ARP 4754 because either the design assurance levels determined using the guidelines would match or any differences determined using DO-254 would be consistent with the overall premise in ARP 4754 of using "the system safety assessment process … to establish and support	Section A: comment accepted. Disposition: delete "its own" from sentence.

	the [system development] assurance level." [SAE ARP 4754, Section D.5] **Comments on Section B: POLICY DERIVATION, Part (1): Main Differences between the Guidelines:** The third paragraph that describes the scope of RTCA DO-254 should acknowledge the Functional Failure Path Analysis and its role in selecting a design assurance level(s) and design assurance strategy(ies) for the specific technology(ies) of the specific functional failure path(s) involved. This is a key aspect of RTCA DO-254 and its application will greatly influence the examples that follow. DO-254 addresses the levels of the functions implemented in hardware, rather than the level of an implementation, whereas DO-178B addresses the level of implementation (software level). The Degree of Rigor description should be expanded to include Level C in addition to Levels A and B to show the rigor applied to the level referenced many times in the examples and to show how it compares to Levels A and B, which are so similar to one another. This distinction for Level C is important because an applicant may seek to reduce the design assurance level for a given function to Level C when it can be justified by the safety assessment in order to use electronic technologies having limited access to design data and to deal with the eventual obsolescence of older technologies. DO-178B and DO-254 modulate between levels in different ways. DO-178B modulates by reducing from the highest level, while DO-254 starts with normal competent processes for Level C and builds on them to get to the confidence needed for Levels	Section B: • Comment on acknowledging the FFPA is accepted. Disposition: revise sentence to say, "The hardware safety assessment, the functional hazard assessment (FHA), the preliminary system safety assessment (PSSA), ~~and~~ the system safety assessment (SSA) processes, and a technique call Functional Failure Path Analysis are used in combination to determine hardware DALs." • Comments on taking level C as the de facto baseline is not accepted. This is not to say the idea does not have merit. It needs to be thoroughly discussed internationally and agreed to by industry before this policy memo can promote it. Disposition: no change to policy memo.

	A and B. DO-178B applies the highest rigor to Level A, and then concedes some rigor for each progressively lower level to modulate between them. DO-254 was built on the idea that what was typically accomplished at the time of its release in a normal and competent state-of-the-art development program is sufficient for Level C [this assumed structured development, requirements-based verification, configuration control, and gathering of the evidence (data and documents)]. The normal processes for Level C are then used as the foundation on which to build up to a Level B or A process. Other important distinctions between RTCA DO-178B and RTCA DO-254 that should be included in this discussion to aid in the understanding of the issues are: • DO-254 differentiates between simple and complex, while the other guidance documents do not. A specific answer to what is simple or complex is not answered in DO-254 because the line is rather subjective based on one's background, and is likely to "move" as technology moves forward. The approach was to acknowledge that a difference exists and to set up a framework for negotiation between the agency and applicant. • DO-254 offers multiple ways to address Level A and B functions, while DO-178B offers only one way (structural coverage analysis). DO-254 makes no preference for any one of the 5 ways, but some methods obviously are more suited to certain electronics technologies than others. These methods are described in Appendix B of DO-254. The idea in DO-254 was to not put forward any preferred method but to accommodate as many as the RTCA/EUROCAE team thought were credible and developed enough at the time,	Other important distinctions…: Although these comments do help better understanding of DO-254, they are not directly pertinent to the purpose of this policy memo. In order to keep the memo short and to the point, these distinctions will not be discussed in the memo. Disposition: no changes.

	and to allow any other method an applicant may propose. This was needed since different technologies lend themselves to different methods. Some of these methods were mentioned (with minimal guidance) in DO-178B Section 12 to indicate their existence but they weren't as refined as they are in DO-254. **Comments on Section B: POLICY DERIVATION, Part (2): Application Examples** Basing most of the examples on the system types presented in SAE ARP 4754 is a reasonable way to compare the 3 guidelines.	
	Examples 1b, 2, 3, and 5 do not have enough specific safety assessment information to determine the DAL as shown and, therefore, do not offer enough information to show the complete distinction of RTCA DO-254. To make these clearer, the consequence of the loss and the malfunction of each individual function need to be presented along with the system effects.	The consequence is the hazard effect; once it is classified the DAL is assigned in accordance to that classification. The comment appears to suggest bypassing the classification in the interests of justifying a lower DAL. This approach could cause confusion in application. If the consequence can be justified to have a low hazard, then the classification should follow suit and DAL assigned accordingly.
	In **Example 1a**, the discussion for DO-254 states there is no guidance for the partition, but the discussions of shared resources in DO-254 Section 2.3.1 and Appendix B provide sufficient guidance for determining the design assurance level of the partition mechanism. The DO-254 column of **Example 2 (should be 1B?)** is not	Example 1a: comment accepted. Disposition: revise the last sentences under the DO-254 column to say: The partition is level B.

	necessarily correct. Although the channels are identical, it is plausible that since Sa and Sb implement independent functions Fa and Fb, the DAL may be exactly as determined using SAE ARP 4754. Further, it is conceivable that both Sa and Sb might be reduced to Level C if more specific FHA information for Fa and Fb is provided. Such determinations may change the summary of the example.	Example 2: the lack of "specific FHA information" does not invalidate this example. Disposition: no changes
	In **Example 2**, if Sx and Sy are truly independent and dissimilar, and if the worst effect from either alone is Major, DO-254 may conclude that these would be Level C, with any common function (perhaps a switching, voting, or fault detection mechanism) at Level A. This highlights the need for specific FHA information and a potential need to identify an additional function, say Sz, for any potentially common function between Sx and Sy so that its DAL can be determined as well.	Example 2: It is conceivable that level C may be acceptable for Sx and Sy (for example Com and Nav systems.) The larger issue is how to apply DO-254 consistently keeping in mind that it is newer than the ARP4754, and both of them have not been thoroughly tested in application. Disposition: revise DO-254 column to say, "Although there may be cases where it might be possible to justify level C for both Sx and Sy, this example will assume the PSSA uses the strategy contained in SAE APR4754 for DAL assignment, Level would be assigned to the hardware of Sx and Sy."
	In **Example 3**, DO-254 would most likely not reach the same result as SAE ARP 4754, mainly because there is no FHA item that is "Hazardous" to correspond to Level B. DO-254 may assign Level C to both Sp and Ss, depending on clarification of the FHA.	Example 3: Because independence cannot be clearly established, as stipulated by the ARP4574, for this architecture, assigning level C may not be appropriate. Disposition: no changes.
	The FHA in **Example 4** appears incorrect, as the effect of a worst-case malfunction of function Sa would be "catastrophic" rather than "hazardous," and it is not clear why the loss of Sm is "Minor" when its result may be a significant reduction in safety	Example 4: to eliminate confusion with the loss of the system which is categorized as Major, the individual effects of Sa and Sm will be revised as follows:

	margins.	Disposition: change classification of -Malfunction of Sa alone to Major -Loss of Sm alone to Major
	There is not sufficient FHA information in **Example 5** to determine the levels per DO-254. The numerical failure rate in the PSSA appears to be from SAE ARP 4754 and its role is not described for determining DAL in the other columns.	Example 5: Clarify that the failure rate comes from the corresponding example in ARP4754. Disposition: change as highlighted: Sa must meet integrity requirements without the backup and must have a very low hardware failure rate – less than 1x10e-7 for loss of function (ref ARP4754 paragraph 5.4.1.5.)
	In **Example 6**, the inspection of a manual switch may not be practical to conduct at such a short interval if it requires removal, but a check of the switch to see if it works may be more practical. Therefore, the word "inspection" should be replaced with "check" in the 4th bullet under "Manual Switch."	Example 6: suggestion accepted. Disposition: Establish ~~an inspection~~ check of the manual switch every 10 flight hours.
	In **Examples 6 and 7**, the System Level FHA discusses software and hardware malfunctions based on an implementation rather than a system level function. Therefore, the 4th and 5th bullets in **Example 6** and the 4th bullet in **Example 7** under "System Level FHA" should be moved to the respective PSSA section and reworded accordingly.	Example 6 and 7: suggestion accepted. Disposition: -Example 6: move 4th and 5th bullets under System Level FHA to the PSSA section. -Example 7: move 4th bullet under System Level FHA to the PSSA section.
	In **Examples 6 and 7**, the top probability of the fault tree represents the probability of the event occurring anywhere in an entire flight. This number should be divided by the flight length to normalize the results to a probability of the event	Example 6 and 7: suggestion accepted. Disposition: -Example 6: also show 5e-13/hr at the top box.

	occurring in a flight hour, as directed by AC 25.1309-1A, paragraph 10.b. In **Example 7**, the monitor channels employ complex electronic hardware, but the 4th bullet under "System Level FHA" describes a software malfunction when there is no software in the system. In addition to moving this point to the PSSA, it should be reworded to reflect the function being implemented in complex electronic hardware rather than software. There is a typo in the fault tree of **Example 7** – the "d" should be removed from "isolated" in the top box.	-Example 7: also show 7.5e-12/hr at the top box. Example 7: There is s/w involved but it is not described in system architecture. Disposition: -Revise sentence as highlighted and moved to "System Architecture": The monitor channels employ software and "complex" electronic hardware. -Correct typo in top box.
Cessna	The activity leading to development of ARP 4754 and DO-254 has been a joint FAA & JAA harmonized activity. It appears that in providing clarification, the FAA may be interpreting the policy in a unilateral manner that is diverging from the JAA interpretations. The FAA should attempt to coordinate this guidance with the JAA and maintain a single FAA/JAA unified position.	The ARP 4754 and DO-254 are industries documents. They are not under authorities controlled. Therefore it is not correct to think of "harmonized activity" between FAA/JAA. Disposition: no changes.
	On page two in the fourth paragraph under "Relevance Past Practice," the FAA comments that it has adopted a similar position for small airplanes with AC 23.1309-1C; however: Part 23 is never again referred to in the rest of the document. Moreover, some of the reliability numbers and hazard classifications are contrary to the guidance in AC 23.1309-1C.	This policy memo is a Transport category paper, as evidenced in its title. The reference to Part 23 applications is for the purpose of reference only. Disposition: no changes.
	Policy section, item 2: Cessna recommends that the last sentence be stricken. The applicant should be able to use this memorandum to show compliance without consulting with the ACO.	An DAL assignment should be reviewed for acceptance by the ACO. Because the paper allows multiple ways of assigning DAL, it is imperative that the ACO understand the method applicants are using. Disposition: no changes.
	Policy item 3: Cessna recommends to strike the sentence, "However, the ACO	Design assurance, in and of itself, is not "fail-safe". It is used when "exhaustive testing may either be impossible

	ASE should recommend the applicant consider a revision of the system architecture to mitigate the potential catastrophic condition." The ACO should determine whether the system complies or not.	because all of the system states cannot be determined or impractical because of the number of tests which must be accomplished." In general, other mitigating means are usually necessary to meet 1309. Disposition: no changes.
	Policy item 4: Cessna recommends to strike everything after the first sentence. Either SAE ARP 4754 is an acceptable standard or it is not.	The ARP 4754 is not a "standard". It is only a guideline and as such its applications need to be reviewed as appropriate to the situation. Disposition: no changes.
	Policy item 6: Cessna recommends to strike "Major" in the first sentence. GAMA maintains that there is little value in applying ARP4754 to "Major" systems.	Policy item 6 addresses usage of DO-254, not ARP 4754. Perhaps there is a typographical error in Cessna's comment. Nevertheless, it is the Transport Standards Staff position that DO-254 should be applied to Major failure conditions due to the decomposition process (Functional Path Analysis) recommended in the document. This decomposition process allows a hazardous or catastrophic condition be "decomposed" into lower DAL items. Not applying DO-254 to Major conditions will result in not applying it to more severe conditions. Disposition: no changes.
	Effect of policy, first paragraph: Cessna recommends to delete everything after the first sentence. The rest has no value added.	The wording are required by Legal Staff to ensure proper understanding and application of the memo within the FAA. Disposition: no changes.
	B. Policy Derivation, second paragraph under Scope: Cessna finds the paragraph confusing, and recommends that the paragraph be rewritten.	Comment accepted. The paragraph will be revise to read: Society of Automobile Engineers ARP4754 was developed from the perspective of complex or highly integrated systems. It excludes specific coverage criteria for validation and verification processes for software and hardware. It only covers those aspects that are of significance in establishing the safety of a system.

		However, it contains examples of DAL assignments to system as well as hardware and software. The philosophy behind its DAL assignments is not always congruent with that of DO-178B.
	Example 1b: The example is not clear. Does Fa provide control and monitor via channel 1 of Sa and channel 2 of Sa? What is the intent of the solid and dashed lines? Does loss of Channel 1 mean loss of monitor? The example implies that this level of detail would be present in the FHA. The FHA would only deal with loss of the function. The guidance of SAE ARP4754 should be allowed to show compliance.	It is clear that Sa implements the function Fa (command)and Sb implements function Fb (monitor). The dash line has the same meaning as the solid line. Loss of channel 1 only remove the redundancy, but the functions are still available via channel 2. The channel failures may not be available during FHA activity. The FHA should cover malfunctions as well as loss of function. ARP4754 is allowed for compliance showing. Disposition: -Change the dash lines to solid lines. -Move the "Failure of Channel 1" and "Failure of Channel 2" from FHA to PSSA.
	Example 6: PSSA, section on Development assurance level determination, third bullet: the word "reliability" needs to be changed to "probability."	Comment accepted. Disposition: change word as recommended by Cessna.
	Example 7 Fault Tree: The fault tree does not include handling of the latent failure of the monitors correctly, per SAE ARP4761, section D.11.1.5.2. SAE ARP4761 has the applicant calculate the "average" probability that the function will fail on a single flight. Example 7 has the applicant calculate the specific probability that the function will fail on the last flight before the inspection.	The correct guidance in ARP4761 is D.11.1.5.2 where 2 items could fail latent. Nevertheless, the intent of the comment is accepted. Disposition: revise fault tree to show average and worst case probability of latent monitor failures.
